Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application. Applicants have submitted a new complete claim set showing marked up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing.

Listing of Claims:

1-33. (Canceled)

34. (New) A dynamic email spam analysis and management system comprising:

a database including a plurality of spam rules, each of the plurality of spam rules having attributes including a score;

a spam analyzer operable to process a log file received from a message switch and operable to update the attributes of at least one of the plurality of spam rules, the updating based on information derived from the log file; and

a select rules file including one or more select rules of the plurality of spam rules, each of the one or more select rules being included in the select rules file based on its attributes, the select rules file being transmitted to the message switch.

35. (New) The system of claim 34 wherein the spam analyzer processes the log file to determine how many times each of the plurality of spam rules was hit and accordingly updates the attributes corresponding to the each of the plurality of spam rules.

36.   (New) The system of claim 34 wherein the attributes corresponding to each of the plurality of spam rules are updated to indicate how many times each of the plurality of spam rules was false-positive-hit.

37.   (New) The system of claim 34 wherein one or more other select rules of the plurality of spam rules are retired, each of the one or more other select rules being retired based on its attributes.

38.   (New) The system of claim 37 wherein the one or more other select rules have not been hit within a predetermined amount of time.

39.   (New) The system of claim 34 wherein the select rules file further includes one or more new rules.

40.   (New) The system of claim 34 wherein the spam analyzer calculates, based on information derived from the log file, how many times each of the plurality of spam rules was hit.

41.   (New) The system of claim 34 wherein the attributes of each of the plurality of spam rules are modified to indicate how many times each of the plurality of spam rules was false-positive-hit.

42.   (New) The system of claim 34 wherein the spam analyzer calculates, based on information derived from the log file, how many hits of each of the plurality of spam rules was determined to be for spam email messages and accordingly modifies the corresponding attributes of the each of the plurality of spam rules.

43. (New) The system of claim 34 wherein the spam analyzer calculates based on information derived from the log file, how many hits of each of the plurality of spam rules was determined to be for non-spam email messages and accordingly modifies the corresponding attributes of the each of the plurality of spam rules.

44. (New) The system of claim 34 wherein the score of one of the plurality of spam rules is modified manually.

45. (New) A dynamic email spam analysis and management system comprising:

a message switch including a spam filter operable to receive an email message; and

a select rules file including a plurality of spam rules usable by the spam filter to analyze the email message and to determine if the email message is a spam email message or a non-spam email message wherein the analyzing includes creating an entry for the email message in a log file, the entry including spam information corresponding to the email message, and wherein the message switch periodically communicates the contents of the log file to a central server and periodically receives an updated select rules file from the central server, the updated select rules file differing from the select rules file, and the updated select rules file becoming the select rules file once received.

46. (New) The system of claim 45 wherein a score is included in the select rules file for each of the plurality of spam rules.

47.   (New) The system of claim 46 wherein a total spam score of the email message is modified using the score of each of the plurality of spam message for which there is a hit on the email message.

48.   (New) The system of claim 47 wherein, if the total spam score exceeds a score threshold, the email message is identified as a spam email message.

49.   (New) The system of claim 45 wherein each of the plurality of spam rules has attributes including one or more of: a score, a date and time the spam rule waslast updated, number of hits, number of spam hits, number of non-spam hits, and date and time of last hit.

50.   (New) The system of claim 47 wherein, if the total spam score does not exceed a score threshold, the email message is identified as a non-spam email message.

51.   (New) The system of claim 50 wherein the email message is transferred to an intended recipient.

52.   (New) The system of claim 45 wherein each of the plurality of spam rules are constructed using regular expressions.

53.   (New) A method for dynamically updating spam rules, the method comprising:

receiving an email message at a message switch;

processing the email message against the spam rules to determine if the email message is a spam email message or a non-spam email message;

creating a spam information entry corresponding to the email message in a log file;

calculating statistics for the spam rules based on the spam information in the log file;

updating a database of the spam rules based on the statistics;

selecting a set of select rules from the database of the spam rules to form a select rules set; and

replicating the select rules set to the message switch wherein the select rules set, once received by the message switch, becomes the spam rules.

54.   (New) The method of claim 53 wherein the message switch is one of a plurality of message switches each operating on a server as part of a distributed network.

55.   (New) The method of claim 53 wherein each of the spam rules has a score.

56.   (New) The method of claim 55 wherein the processing includes testing the email message against each of the spam rules for a hit and, if a hit exists for the each of the spam rules, modifying a total spam score of the email message based on the score of the each of the spam rules.

57.   (New) The method of claim 56 wherein the spam information entry corresponding to the email message in the log file includes an identifier for each of the spam rules for which there was a hit.

58.   (New) The method of claim 53 wherein the calculating includes calculating, based on the log file, how many times each of the spam rules was hit.

59.   (New) The method of claim 53 wherein the calculating includes calculating, based on the log file, how many hits for each of the spam rules were for a spam email message versus a non-spam email message.

60.   (New) The method of claim 53 wherein the updating includes updating a quantity of false-positive-hits for one or more of the spam rules.

61.   (New) The method of claim 53 wherein the selecting includes retiring one or more of the spam rules wherein the retired spam rules are not included in the select rules set.

62.   (New) The method of claim 55 wherein the updating includes updating the score of one or more of the spam rules based on the statistics.

63.   (New) The method of claim 55 wherein the score of each of the spam rules can be modified manually.

64.   (New) The method of claim 54 wherein the replicating includes replicating the select rules set to each of the plurality of message switches.

65.   (New) The method of claim 53 further comprising, if the email message is determined to be a non-spam email message, transferring the email message to an intended recipient.

66.   (New) The method of claim 53 embodied as computer-executable instructions stored on a computer-readable medium.